What is claimed is:

1. A copy protection method for digital media, the method comprising the steps of:

(a) encrypting an original media data set with a media key corresponding to a symmetric algorithm and encrypting said media key with a public key of a compliant playing device;

(b) delivering said media data set and media key encrypted in the step (a) and a media certificate to said playing device, said certificate including a private-key identification of said playing device, said private-key identification being encrypted with said public key;

(c) decrypting said private-key identification;

(d) searching for an actual private key by checking whether each of stored private keys of said playing device corresponds to said decrypted private-key identification;

(e) decrypting said delivered media key with said actual private key; and

(f) decrypting said delivered media data set with said decrypted media key.

2. The method of claim 1, wherein said stored private keys include a current private key and one or more old private keys,

each of said old private keys being previously revoked through a key revocation process.

3. The method of claim 2, wherein said playing device includes a rewritable memory storing said old private keys.

4. The method of claim 3, wherein said older private keys being stored in said memory are encrypted with said public key.

5. A copy protection system for digital media, the system comprising:

a private key verifier receiving a media certificate that includes a private-key identification of a compliant playing device and searching for an actual private key by checking whether each of available private keys of said playing device corresponds to said private-key identification;

a media key decryptor receiving an encrypted media key and decrypting said media key with said actual private key; and

a media data decryptor receiving an encrypted media data set and decrypting said media data set with said decrypted media key.

6. The system of claim 5, wherein said available private keys include a current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

7. The system of claim 6, further comprising a data-rewritable memory storing said one or more old private keys.

8. The system of claim 7, where said older private keys being stored in said memory are encrypted with a public key of said playing device.

9. The system of claim 5, wherein said encrypted media key is encrypted with a public key of said playing device.

10. The system of claim 5, wherein said encrypted media data set is encrypted with an original media key.